

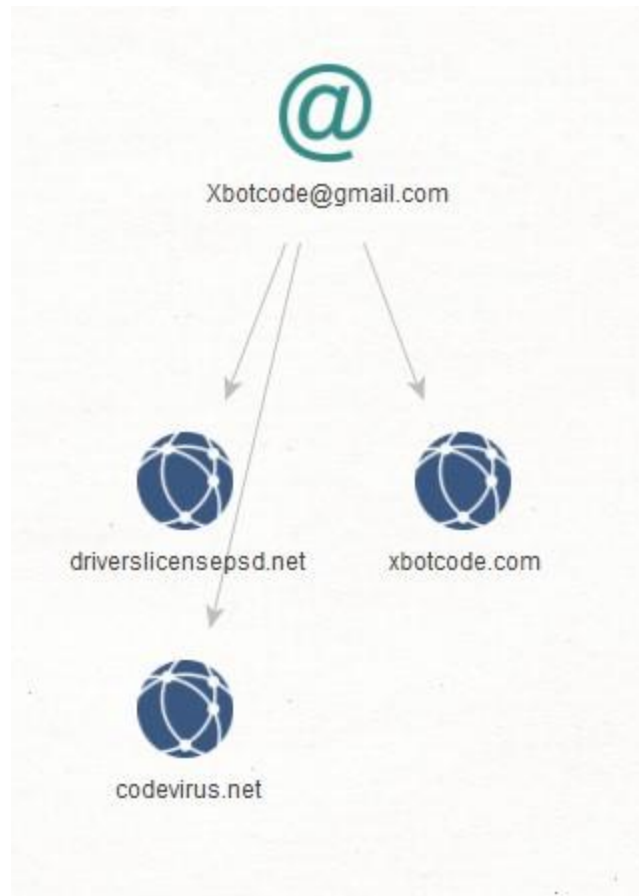
00. Exposing a Currently Active Domains Portfolio of Known to Have Been Used by Ransomware Network Affiliate Based Participants Including Ransomware Gang Affiliates - An OSINT Analysis



Wonder what are the primary domain properties of publicly known and confirmed ransomware affiliate network based revenue-sharing participants?

In this analysis we've decided to use personally identifiable information which belongs to various ransomware network participants with the idea to use WhoisXML API's vast current real-time and historical WHOIS database and try to offer more actionable intelligence on the actual domain properties known to belong to various ransomware gang affiliate network revenue-sharing network's schema in order to assist U.S Law Enforcement on its way to properly track down and monitor these individuals.

We'll also detail in-depth the activities of a known ransomware gang's participant that is also known to be currently selling and offering access to fake documents and driving licenses including the actual source code for his ransomware including access to the actual service.



Sample domains known to have been involved in the campaign and currently in use by various ransomware gang members include:

badfail.info
watchabag.com
exchanger-cash.com
driverslicensepsd.net
sunrisekidsindia.com
sqeets.com
irancybp.ir
codevirus.net
watchabag.com
ecotokens.su
exchanger-cash.com
driverslicensepsd.net
xbotcode.com
sqeets.com
codevirus.net
wheelipedia.com
truongquocvi.info
truongquocvi.com

giwebsolutions.in
vietonl.net
softfilemanage.com
a6tdn.com
decode-india.com
agendas-personalizadas.com
elitemenu.xyz
lixiongchen.com
shelbysdatenight.com
badfail.info
gotocosplay.com
irancybp.ir
angiesensei.com

What we initially found during our analysis was a well known to have been involved in various ransomware campaigns email address account that is also known to have registered a fake documents and driving license's service domain including an actual domain and is currently active and is selling access to the source code of the author's ransomware including access to the actual service.

Email address involved: Xbotcode@gmail.com

Domains involved: driverslicensepsd.net; xbotcode.com; codevirus.net

1. Source Code Decrypter Ransomware

This is Source Code to build a Decrypter Tool. You can custom with your info. Free support how to setup and Compile Code.

2. Code Macro Microsoft Office (Word, Excel)

This Code inject to Microsoft Office. Example: Exe + Doc = Doc (.exe file run when open Microsoft Office).

3. Code Macro Javascript Bash (.js)

This code include automatic (silent) download and open a file (.exe) after victim download a .js file (bypass AntiVirus Program) - Free update weekly.

4. Code Update Virus Program

Code build an exe file simple. Main function is bypass Antivirus and Start when Windows Start. This file is normal program, not virus.

5. Support (Setup C&C;, SMTP Server,...)

This service free setup C&C; Server, SMTP Server for SPAM large email, Configurate Server, IP, Domain DNS,...(Free support 1 year).

6. Setup .Onion & Gateway (Bitcoin, PM)

This service will help you setting up a domain with TOR service. You will hidden on Internet. I will help to support create Gateway payment via Bitcoin and Perfect Money too.

According to the ransomware author's web site some of the features of his ransomware include:

- Small Program
- Process run hidden
- Encrypt with RSA-2048 bit (very strong)
- Send Decrypt key to your email
- File encrypted can not restore if don't have Key
- Custom any icon (like: IDM, Adobe Flash,...)
- Works with all Windows version (XP, 7, 8, 10, 2003 Server,...)
- Clear FUD, Bypass UAC

Announcements (September 12, 2022)

- Add new and update all passports, national id, driver license, bank statement....all countries in the world.
- We are updating daily new template PSD file, send an request to me set priority country and sample. [Click here to make a request!](#)
- We are accept Bitcoin and Altcoin (cryptocurrency only).
- Support email: support@driverslicensepsd.com

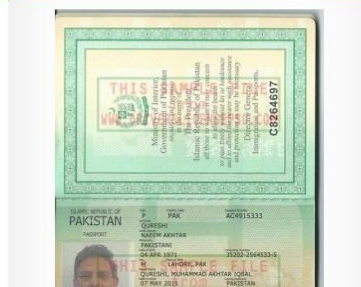
Most Recent Products



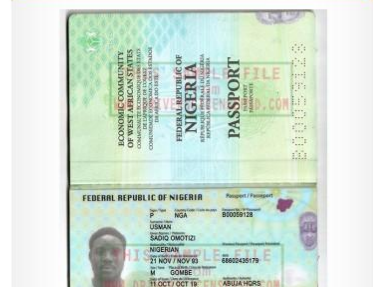
United Kingdom of Great Britain and Northern Ireland ...



Pakistan Passport 01 PSD



Nigeria Passport 01 PSD



Addon (Source Code Ransomware)

1. Source Code Decrypter Ransomware - \$95
2. Code Macro Microsoft Office (Word, Excel) - \$30
3. Code Macro Javascript Bash (.js) - \$30
4. Code Update Virus Program - \$49
5. Support (Setup C&C, SMTP Server,...) - \$99
6. Setup .Onion & Gateway (Bitcoin, PM) - \$149

Sample responding IPs known to have been involved in the campaign include:

104.31.66.72
206.72.201.76
172.67.163.206
77.73.68.126
104.28.30.236
185.145.131.166
172.64.80.1
104.31.67.72
209.99.40.226
146.112.61.108
104.18.43.120
104.18.42.120
44.227.76.166
209.99.40.221
192.187.111.220
31.170.161.28
54.65.172.3
50.63.202.93
104.24.119.50
198.61.166.153
64.31.42.235
69.172.201.153
207.174.213.34
66.96.147.120
185.212.130.15
195.54.163.133
64.31.42.236
34.98.99.30

85.208.114.180
162.215.226.3
194.58.56.192
123.30.250.119
104.27.151.200
104.239.213.7
194.58.56.102
104.28.2.87
188.227.75.186
188.114.96.21
31.170.160.61
27.254.87.155
209.99.40.225
209.99.40.223
87.107.172.29
208.73.211.235
208.73.211.179
212.227.165.70
208.73.211.195
209.99.40.222
74.119.239.234
217.160.31.116
217.160.237.194
208.73.210.217
208.73.210.211
208.91.199.224
208.91.199.116
47.91.202.66
208.91.199.246
47.88.84.51
185.181.104.82
156.238.54.201
69.49.101.233
208.91.198.143
208.91.199.6
1.52.29.236
115.76.181.39
182.74.236.10
116.108.216.114
182.74.236.5
27.78.39.191
64.74.223.42
116.108.27.17
23.195.69.108

104.27.134.140
184.168.221.87
104.194.231.24
104.131.203.73
184.168.221.65
104.27.135.140
184.168.221.70
172.64.81.86
104.28.31.236

We've also identified the following malicious MD5s known to have phoned back to the same responding IPs as the actual hosting location of the original domains known to have been involved in this campaign:

eabe3ec91d70a41e704a49e70a2dade0
90e83959c57aaa8e9cb086e9175669fa
ddd6ca28c607a4b69849e378f9b66394
4e4272a15ef08453494f597accfa5c6c
1485dca59636bd5756e1858384330321
31504199e9f2b99816aff3f154e55ca1
c34c2493a05d7ad43809e6431af5e04a
0aecfda7b1e0ae3833db5b5424012813
59dbb9121ad795a41b1c303e6167bdd8
81cd1c0275cc5a755dc21a4d84d5a647
b4cce83d72f4cde44996f6d912b1c274
9141dc9c2a0ff0ac7832d29c969a0b48
b9eda89e78fab8b35f59c667b4d0990
91adad8a9b13ca671b0fd6bf22a15af1
1e1c7ee49ee3595c70b0092a7613c1b9
a04b1a6fe0b062727b6acf0309debba1
c05f58b49a3fdf12fc21316053db55f8
52dc4806e51e63a7343c84967eaaac13
9500bcbf312b35e6494ae73d7c03893f
e2a3cfd9daf348a7ec75b45646c8a11d
b009bb06d7ab92407d40839d9d22fb07
373c849ee7d2e6324a2ac1b8c8d5f095
8f0373b7dd7142bf62ed656026455c41
d260a24ffa3cb33fd703f6ca88bbfcf6
da92d4ac9d27a33a76af44aaed78a614
c9dc8bc198e091102f250015c8c4f00c
fa0d82ed48cb19ad9767142fad906ebf
63c0744b6613baf858e83b396ae31dd2
8c9089bb6a4b0b9db16c1c8c8c665b7c
53751ee70ff66d812108e3378b77b720

ef91e58024cb1b19a119c61770f5fc0d
abac0b10defa14335d556ddfde76bdaf
bb6db298e50799c14cc4526b80e1f050
f008ba12458221e49042e4277a6e3aec
62838cf450a8c0de31a0cab4a87ca205
c79625de05edf1d9476ec74656eaae79
17bd603976bf2ff54ba60c500a7103bc
c3169a21edd61ef5906df4bc7a65fd12
ef750c40f2cad86d5875986bff181abb
2a4caed9f32e4ba905df8913318e551f
cb91827a9a47d4acdc52d711fa169025
2ee9304765c85dc60b384bc2542ddc9a
91211eeb15a9eaaf64c6c237e5117046
697e91957882aeb73b0262738a9909ab
8ceb8fae93a26170fae36b06e4ef1e16
a8dce81aff27a61ff30b94528c5afa63
010aedfee95b05b74f139d0257b44e4c
18c6622ca845d0f1653caeb194c579f6
04c88d3616c46398a39adab91228ae87
588293ff2639a873b310a61a68be27f7
e0b3a8d66ea911d0f80381b095238f32
f4c167d7cf9c8aa4402215292a2dfab2
af50076614e5eb68c5a663d82c55c350
19d57acae0fcdcbff3fe0fb704c0d25e
bb9b69f5e2af72a9fa63a76929550ec9
1b7554cb715f0a2dce1b3e2f07d4b4af
cbef9bb5f4b4bf986d0cfdab2f1ac737
e2a997b862cb76d5e33fa4eafde84d55
6a9104f52c0aee59338bacc65920e9bd
f45b9497fd30bce8dc17641cc56c7444
c1114623247e7392f97b54998e4fc32c
34d762c7a9e6bc6958109212f70081f3
b43d2e0be5c479937bee17bb89e0661e
1f109d5e1fb5f989da4bad2ba262f483
68451b52d8d39148114b0763518387db
39fc5cf0906d690daaad9fe14e17d2fb
ffe56bb2f6d807c0df683a7056a6e0d0
622a4d29db1c7d5ad5ab359e572bb9c0
2936829d6ab21783ef9f3758c732b3f1
ae32492a7f95ad36f899e68fb85e3afb
3d3622ba9c645a8f19ca8879120c0263
f71ec952aa13800d7c537043cd405a99
cea6f8d6cb6e8e3d0beda17b55cf7348
bf023e2f5654459f0885ffa562656718

6dd6698f4c91090ed82bbc0cdbba78b6
466d71772009000eff3178988baa8a57
29249a7bd3c116a349607334e3d8ac4c
d72a8c4a47dd37dd4ae151b01c86f8d5
3fabf9969ba7085b39eedf1b15a783d6
54d065f4d2bd7d2401ac2fad5bef72d8
4053a409852607a8bd145dafad33bbe3
13c58bd63cdebbb37f6fc73dedce737f
9872c1bd237dc1a4a973421d5d13aec1
b531f73eaa6255e7a7c242bdcfb39061
00c7bdfc5c01bb3c0ab9fc9e2886c8a7
8cde74b959218cb5d05b113587de70ce
faccf5230cc7e4ed9319139e16fd3786
2a7cf3f375ed5da14b3cb540cea442ee
7f3903597a5d6e3c5223c9079d75abd3
b12ee46fe25a4c38a0ad23992676745b
26c409d03d3adeba2757446236ee9384
6689cbb8f4efd05d91a5d7b02480a4d1
af1a38cd6ce6014a59155c1663b015d3
59654d3b910b5fa2848eab53d02547fd
242e96fdfca5cdb3f4ff1f3fe237c006
9c138b0b529b98d58d08d5f80ff950b7
49ece2a6a3c42f2afd0811c66b3e3a85
1b2d2f100fca7a242d3d2123df43a92e
90874f05de97450d17beda5ad47ea0e2
de92d12a3fcf4c65e1a7fb4112da5171
ae0d66ab71d4efd3e08752eae1d3e426

We'll continue monitoring the campaign and will post updates as soon as new developments take place.